(12) UK Patent Application (19) GB (11) 2 154 832 A

(43) Application published 11 Sep 1985

(21) Application No 8501738

(22) Date of filing 23 Jan 1985

(30) Priority data
(31) 8404562 (32) 21 Feb 1984 (33) GB

(51) INT CL⁴
H04B 1/59 5/00

(52) Domestic classification
H4L GA
G4Q CB
G4T AX
U1S 1819 2133 G4Q G4T H4L

(56) Documents cited
GB 1573183 GB 1507050 GB 1462055
GB 1573111 GB 1488850

(58) Field of search
H4L

(71) Applicant
The Plessey Company plc (United Kingdom),
Vicarage Lane, Ilford, Essex IG1 4AQ

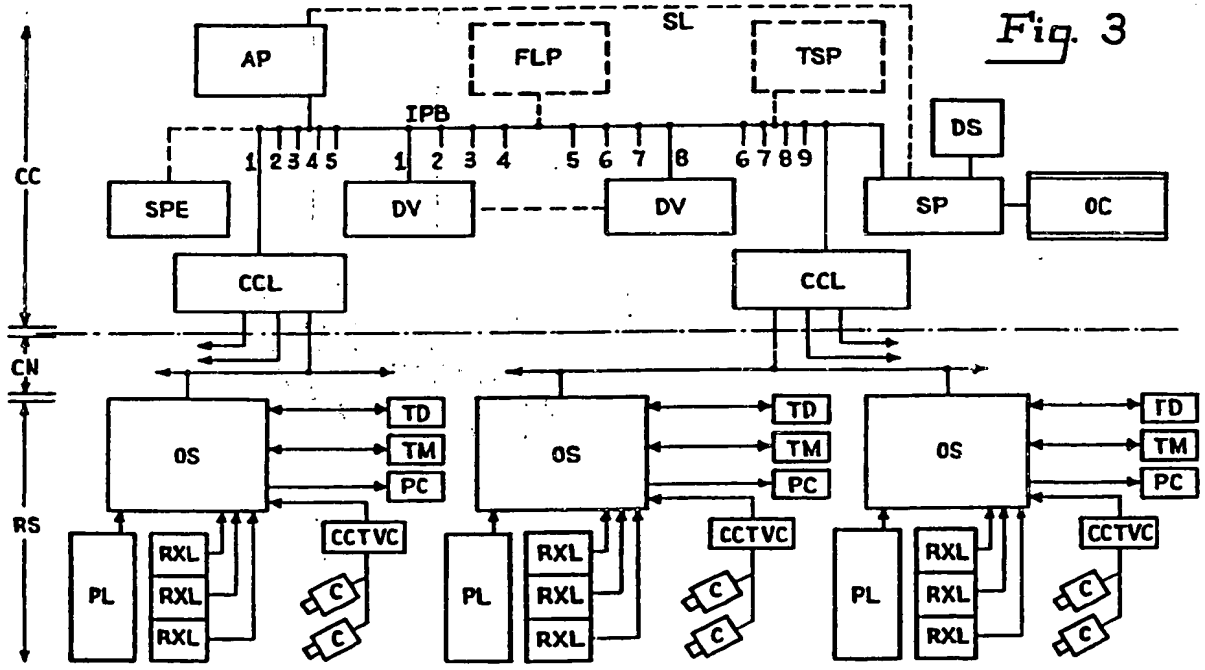
(72) Inventor
John Dyson Turner

(74) Agent and/or Address for Service
H J Field,
The Plessey Company plc, Vicarage Lane, Ilford, Essex
IG1 4AQ

(54) Data capture system

(57) The system involves the fitting of Electronic Number Plates (ENP's) to all road vehicles with roadside interrogators (outstations OS) and central control equipment to collect and validate vehicle identity data before passing it on to an accounts processing system AP. The system is organised so that there are a number of vehicle data processing devices (Data Validators DV) which receive data from the outstation units (OS) interrogated by a communications controller (CCL). Each Data Validator (DV) is allocated a discrete subset of all vehicles in the system to enable vehicle location checking to be maintained as the vehicles move through the system. Any apparent error in vehicle data is passed on to a supervisory processor which checks if the error can be explained. This provides a powerful vehicle location consistancy check and fraud identification system allowing speedy detection of fraud, stolen cars or electronic number plates.

Fig. 3



GB 2 154 832 A

2154832

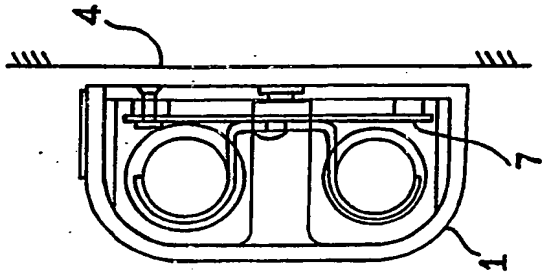


Fig 2

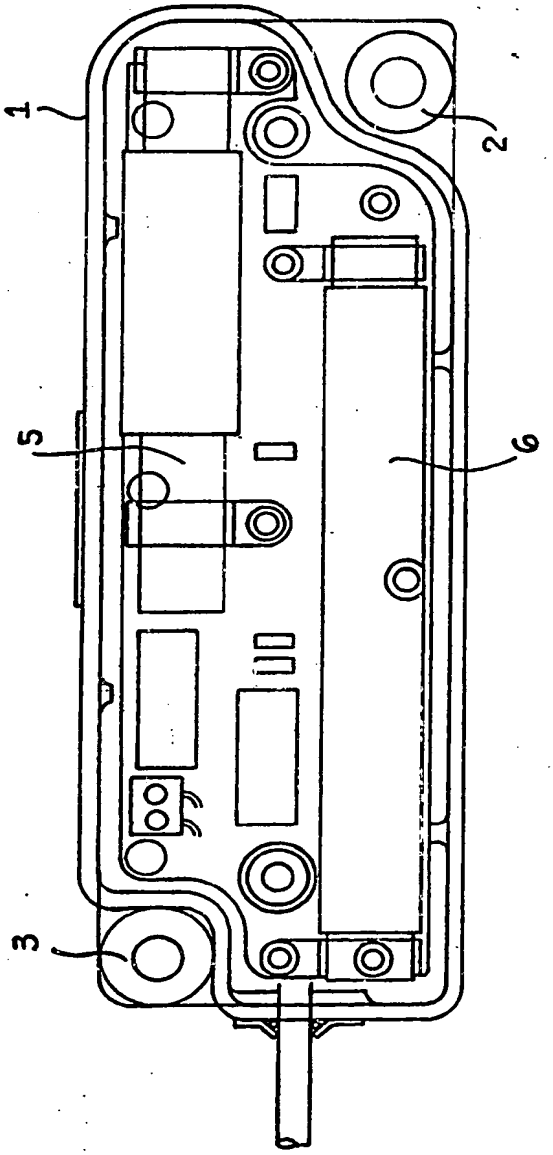
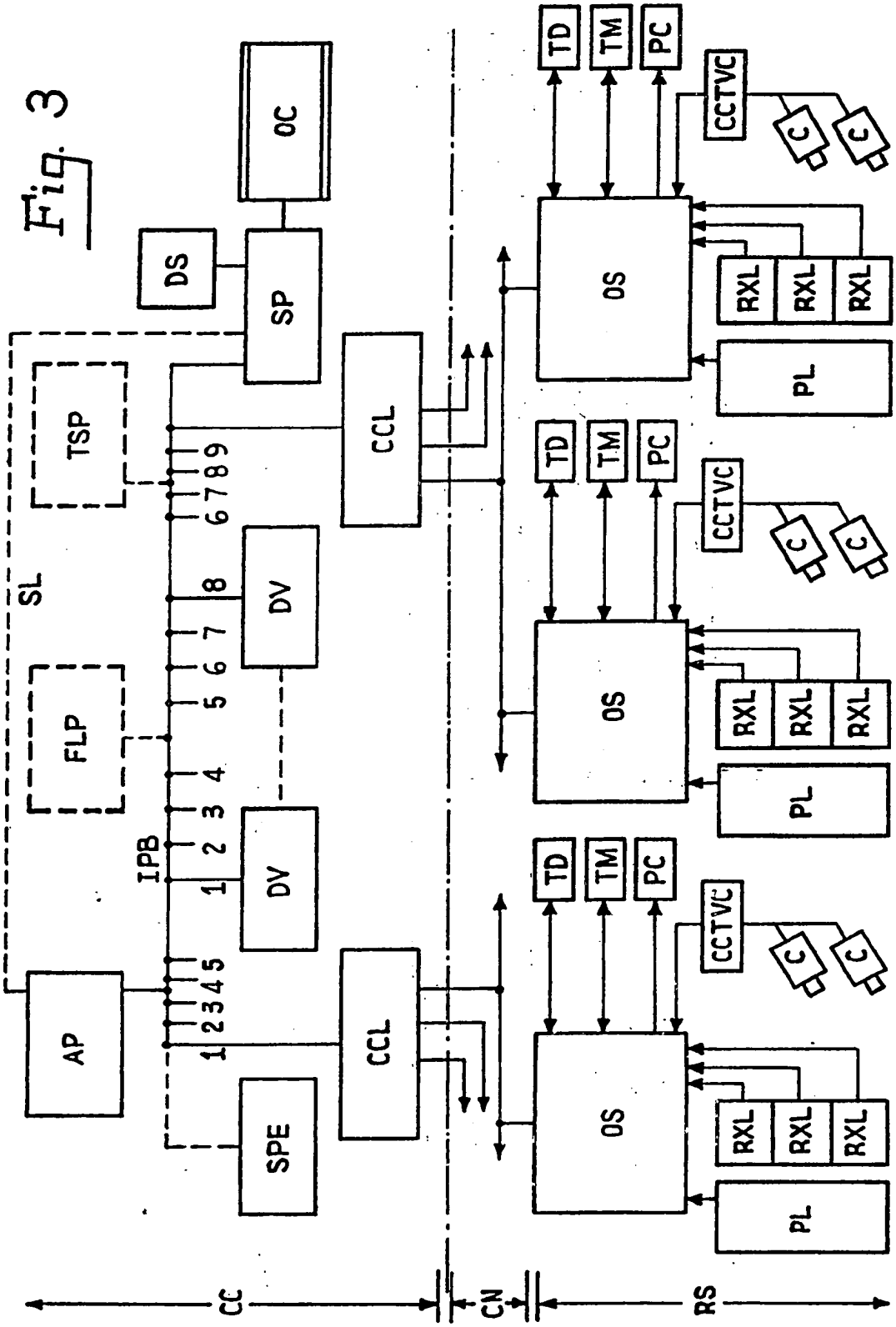


Fig. 1

Fig. 3



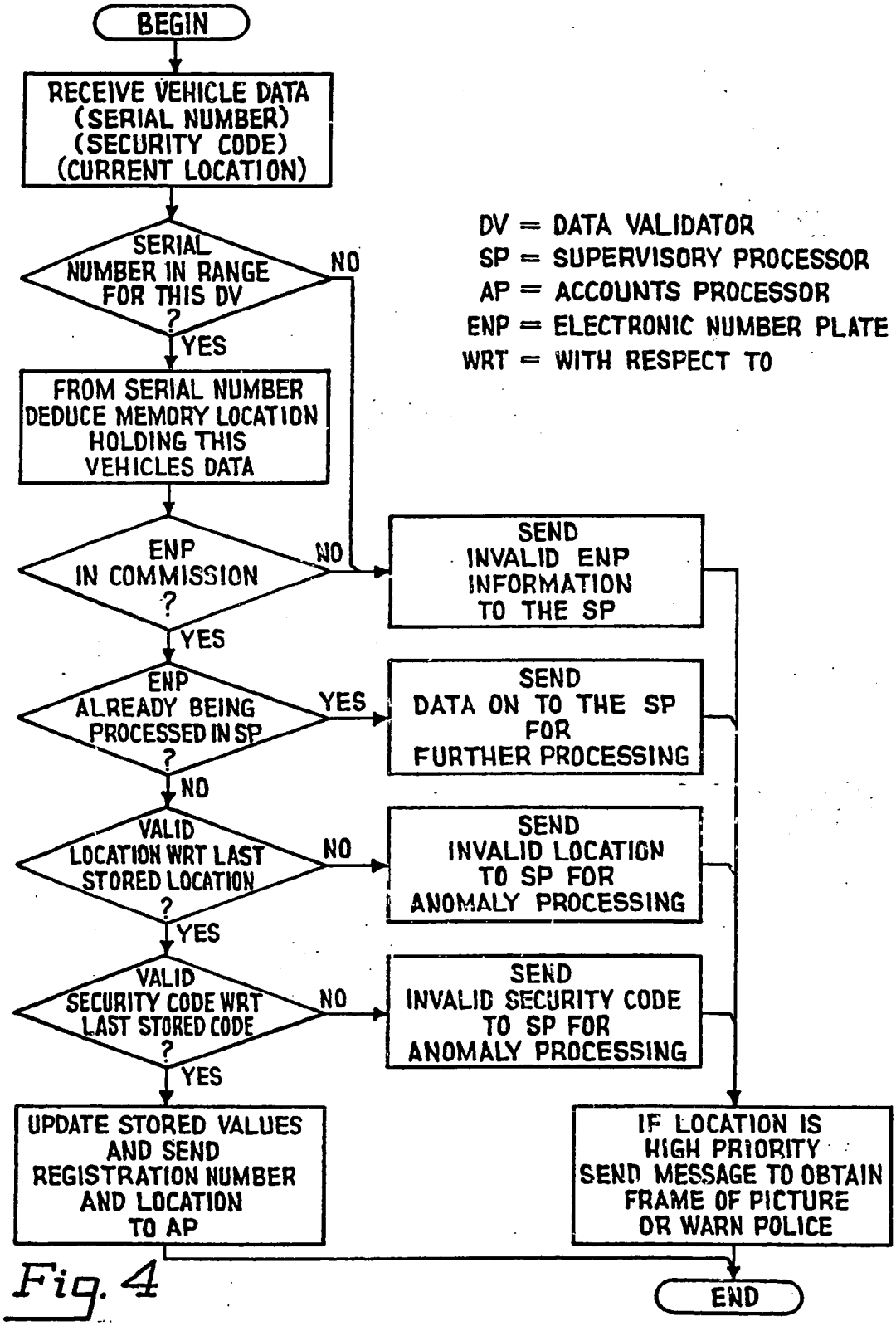


Fig. 4

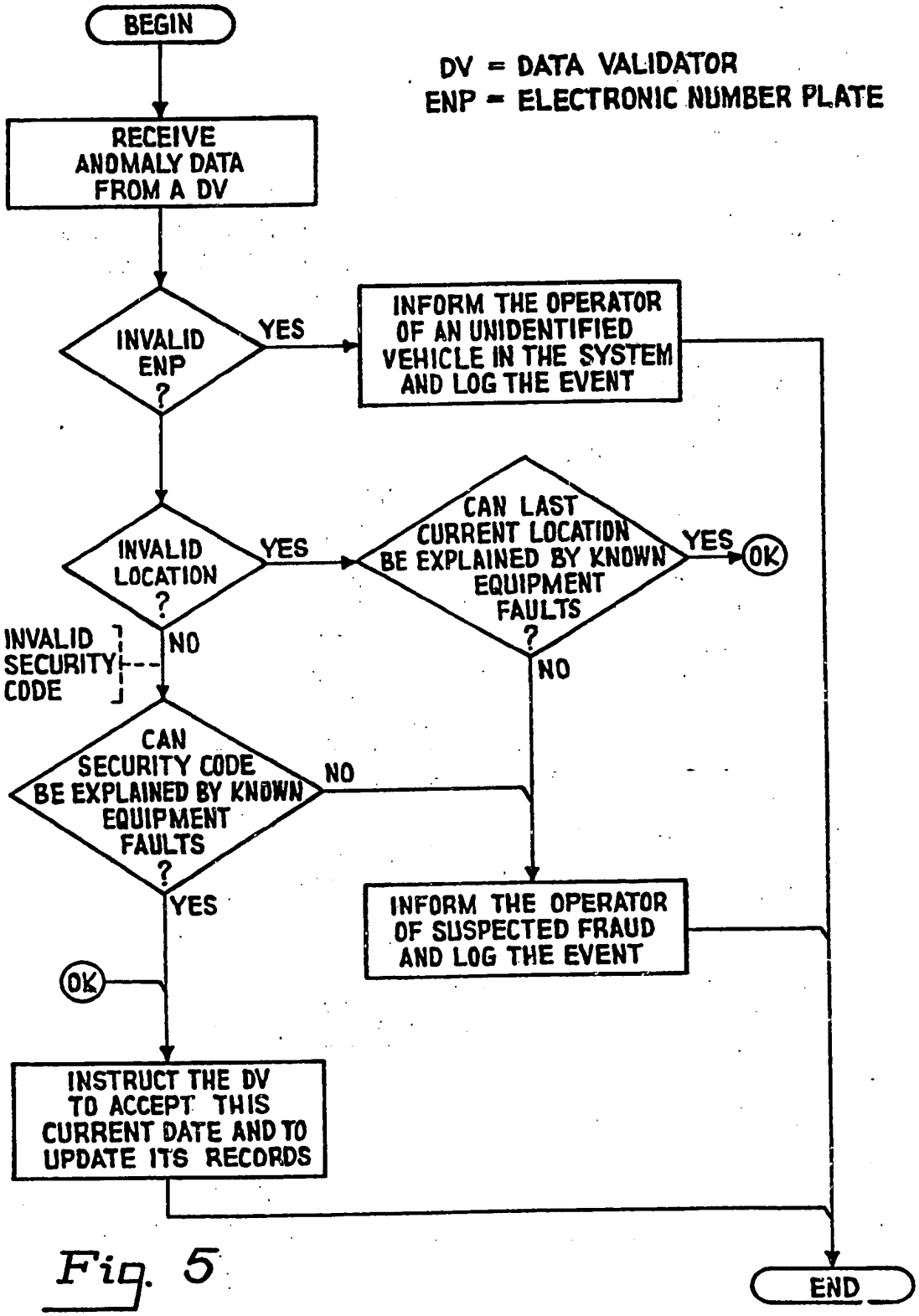


Fig. 5

SPECIFICATION

Data capture system

This invention relates to a data capture system for the automatic charging of tolls to vehicular users of roads.

According to the present invention there is provided a data capture system for the automatic charging of tolls to vehicular users of roads, the capture system comprising, a plurality of vehicle identity data transmitting means each being individually attachable to vehicles, a plurality of roadside vehicle identity data interrogating means linked by a communications network with a central control which includes a plurality of communications control processors, and a plurality of vehicle identity data validating processors which communicate by means of a common inter-processor bus, wherein each data validating processor is allocated a discrete subset of all vehicles handled by the system and wherein upon transmitted vehicle identity data being detected by any one roadside vehicle identity data interrogating means, the vehicle identity data is transmitted through the communications network to a communications control processor and then by way of the common inter-processor bus to the particular data validating processor allocated to the subset of vehicles within which, the detected vehicle identity data is located, whereupon, the detected vehicle identity data is validated for use in enabling the preparation of toll invoices for despatch to the particular vehicle user concerned.

The invention will be better understood from the following description of an exemplary embodiment which should be read in conjunction with the accompanying drawings, in which:

Figure 1 shows a plan-view of the apparatus which comprises an electronic number plate;

Figure 2 shows a side-view of the apparatus shown in Figure 1;

Figure 3 shows a block schematic of the data capture system in accordance with the invention;

Figure 4 shows a flow diagram for the data validation processing;

Figure 5 shows a flow diagram for the anomaly processing/fraud identification for the supervisory processor.

The data capture system comprises electronic number plates (ENPs) fitted to road vehicles, roadside interrogators, data transmission equipment and central office equipment to collect and validate vehicle identity data before passing it on to an accounts processing system.

ELECTRONIC NUMBER PLATE (ENP)

Referring now to the drawings; each vehicle in the system is fitted with vehicle identity data transmitting means or electronic number plate (ENP).

The ENP 1, (as shown in Figure 1 and Figure 2), is a small sealed module approximately 200mm long × 75mm wide and 40mm deep. It is located by means of securing points 2 and 3 beneath vehicle body 4. It is easy to fit, but once fitted is difficult to remove.

Each ENP apparatus has a unique identifying serial number which is converted into code and stored in the ENP apparatus during manufacture. All ENP apparatus codes are independent of any vehicle mechanical registration number, making it difficult to copy and defraud.

At the fitting station where the vehicle is equipped, the vehicle registration number is entered into the system by an operator via a keypad, whilst the serial number is read automatically into the system by an interrogator. This serial number is not displayed to the operator, for security reasons. The ENP apparatus is equipped with two aerials 5 and 6 which provide electromagnetic coupling with inductive road loops (cables buried in the road). One aerial receives sufficient energy to power up the ENP apparatus when it is in the immediate vicinity of a power loop PL. This aerial also provides a clock input for the ENP circuits which generate the synchronous data to be transmitted via the other aerial back to a receive loop RXL.

The ENP apparatus receives its power and clock at 147kHz and transmits the data on a 73.5kHz carrier. The data rate is 9.1875kBaud, i.e. one sixteenth of the powering frequency.

The ENP apparatus contains three integrated circuits (IC's). One, a fuse-link PROM, is programmed with the serial number code during manufacture. Another, a CMOS custom IC performs all logic functions, and a special bipolar IC, measures signal thresholds and performs the linear functions. These IC's, together with other components, are mounted on a printed circuit board 7.

The ENP apparatus is capable of transmitting the serial code (in phase modulated form), a security or check code for providing an extra protection against fraud, and (optionally) variable data set-up by the driver of the vehicle on a variable data unit within the vehicle.

Various types of variable data unit's can be used. Some of the data field being varied automatically by peripheral equipment connected via the unit. This may include such items as emergency vehicle status and priority code, bus identification, depot, fleet and route number. The remainder of the data field being varied by switches on the unit.

OUTSTATIONS

Along the roadside RS are located vehicle

identity interrogating means or outstations OS which comprise an interrogator, which is connected to the inductive road loops (power PL and receive RX), a processor, a transmission unit and a number of interfaces to local equipment, such as a toll display TD where charges are indicated, a closed circuit television control CCTVC, a maintenance handset or terminal TM through which police and maintenance services gain access to information, and a priority controller PC for handling control signals relating to vehicles requiring priority.

CCTV SYSTEM

The CCTV system includes cameras C at certain roadside interrogation points (outstation OS) which store pictures of vehicles in a category termed suspect, for onward transmission to the central control CC for analysis. A suspect vehicle could be one for which no identity data is received, one where the security code or location is found to be inconsistent, or one wanted by the police, for example a stolen vehicle. A list of suspect vehicles (the 'Wanted List') is held by the supervisory processor SP at the central control CC.

SYSTEM IN GENERAL

It is arranged for the interrogator to demodulate signals received from each receive loop RX and pass the identity data to the processor where the code is verified. Vehicle identity data are subsequently transmitted from the outstations OS by the transmission unit, central control CC by way of a communications network CN in the form of cable network. Each communications controller CCL has control of a part of the complete cable network, with a number of outstations (e.g. ten) connected (via the network) to each of its communications channels. The central control CC comprises a number of communications controllers CCL, a number of processors (accounts processor AP, Supervisory processor SP, fleet location processor FLP, traffic statistics processor TSP, data validation processor or data validator DV, and a spare processor SPE), disc and tape storage, and operator communication facilities OC which include visual display units (VDU's) and a hard copy terminal or printer.

The communications controllers CC, handle data transmission between the outstations and a high speed bus IPB to which all the central control processors are connected. The IPB is a local area network link arrangement termed an ETHERNET bus which operates 10 Mbits over a single coaxial cable. Processors tap into the cable at intervals allowing up to 100 stations (nodes) on a 500m cable with up to 1024 stations in any network.

Concerning the various processors mentioned above, the data validation processors or data validators DV check the security code (if used) and location (outstation) of each ENP against the last known interrogation data, an accounts processor AP, prepares road charge invoices and despatches these periodically to the vehicle owners and a supervisory processor SP oversees the operation of the data validators DV, co-ordinates fault detection and recovery, including checking if apparent errors in vehicle data can be explained by faults known to the system ('Anomaly Processing'), and handles operator communications.

Data received from the outstation units OS are interrogated by the associated communications controller CC and passed to the appropriate data validator DV via the high speed bus (local area communications network IPB). Each data validator DV is allocated a discrete subset of all vehicles in the system, to enable vehicle location checking to be maintained as the vehicles move through the area, and are detected by the different outstation units OS and, hence, different communications controllers CC.

Any apparent error in vehicle data is passed on to the supervisory processor SP, which checks if the error can be explained by known faults in the system, such as a faulty upstream interrogator. At the same time, if the vehicle was detected at a manned or CCTV outstation, data is sent to that outstation for display on the local terminal or inclusion with display at the central control. Valid vehicle data is output for use by the accounts processor AP.

Data that fails the validity check and anomaly analysis causes that ENP to be marked as 'suspect' in the computer records. It is added to the 'Wanted List' in the supervisory processor SP and marked for special attention in the data validator DV responsible for that ENP.

COMMUNICATION CONTROLLERS

Referring to the Communications Controllers CCL these poll each outstation in turn to retrieve the vehicle information. Any control information being sent from the central control CC to an outstation OS is included in the appropriate poll request frame. The protocol adopted permits messages to be sent from the communication controllers CCL to all units on a line. The protocol used is the internationally agreed standard for High Level Data Link Control Procedures (HDLC). The main function of the communication controller CCL is to buffer the individual vehicle information for onward transmission to the data validators DV. It determines from each vehicle's ENP code which data validator DV is the required destination. (It should be noted that there are several data validators DV each processing a subset of all vehicles in the system). The communication controller CCL sets up output buffers accordingly and then sends the data to the destination(s).

TRANSFER OF DATA (OUTSTATION TO CEN-

TRAL OFFICE)

Priority is given to any outstation unit which is connected to CCTV equipment or which has a terminal connected to it; for these sites, information from the outstation may elicit a response from the central control. Usually the response will relate directly to a vehicle passing the site, so it is essential to get the response to the outstation quickly (before the CCTV equipment overwrites a stored picture frame with another picture, or before the vehicle has moved too far away from a manual site to permit police intervention). Consequently these sites are marked as 'high priority' and will be polled by a communication controller CCL at about twice per second, interrupting the sequential polling of each of the other (low priority) outstations.

As an outstation only transmits information to the central control when asked to do so by a communication controller CCL, different types of information can be combined into one data packet, depending upon what is requested by a communication controller the current status of the equipment at the outstation at the time of polling. These types include:

a) Vehicle ENP data;
b) Site and lane identification, per set of ENP data;
c) Fault indications;
d) Toll charge confirmation;
e) Whether a terminal is connected to the outstation's handset port;
f) Messages and/or commands from the terminal; and
g) The results of a 'self check' by the outstation processor.

Note that these types are for standard outstations operating manually. In addition to these, outstation initialisation involves several 'supervisory' data packets to set up the link to a communicaions controller CCL and acknowledge completion of the initialisation process.

As a communication controller CCL receives outstation data packets, it sends vehicle ENP information to the data validators DV and all other information to the supervisory processor SP. For each set of ENP information, the vehicle's ENP serial number is used to identify which data validator DV holds its current location (and security code, if any) and different data packets are set up to send to each data validator DV. High priority site data is separated from low priority site data so that the data validator DV is synchronised to the end of polling of the high priority outstations.

TRANSFER OF DATA (CENTRAL OFFICE TO OUTSTATION)

The normal data transmitted from a communication controller CCL to an outstation is a poll for vehicle ENP data. The following items may be incorporated within the 'poll request' packet:

a) Toll charge updates;
b) Equipment fault clearance;
c) Instructions to outstation units to perform self check;
d) Requests for self check test results;
e) Replies to messages/commands input from the engineer's terminal; and
f) Confirmation of vehicle commissioning.

The following items are interleaved with the poll request packets:

a) Outstation initialisation and down line loading information; and
b) 'Wanted Vehicle' requests.

HDLC PROTOCOL

As each outstation OS communicates with a single communications controller CC, the operating mode for the links is that of primary-secondary polling. The communication controller CCL acts as the primary (master) station and the outstations on each link as the secondary (slave) stations.

Each communication controller CCL outstation 'link' is set-up for frame transmission and messages are passed in the form of a header (made up of the required outstation address and control information), an information field and a frame check sequence. As the message is received, the frame check sequence is recomputed and checked against the frame check sequence at the end of the message. If the frame check sequence is correct, an acknowledgement is included in the next frame to be sent in the opposite direction. This mechanism allows for re-transmission of unacknowledged messages, thus increasing the reliability of data transfers throughout the network.

MESSAGE HANDLING (OUTSTATION)

For each link under its control, the communication controller CCL cycles around each outstation OS under the control of two lists. All low priority outstations are contained in one list and the communication controller CCL cycles around them, polling for vehicle ENP data, unless interrupted by a higher priority item i.e., a high priority outstation poll, a wanted vehicle request or initialisation/down-line loading of an outstation. The last two items are random whereas the high priority outstation poll is under the full control of the communication controller CCL. Each half-second, the communication controller CCL polling task will be flagged to use the high priority outstation list—breaking into the low priority cycle. When all high priority sites have been polled, the communication controller CC reverts to the low priority cycle again.

MESSAGE HANDLING—(CENTRAL OFFICE)

As messages are received over the HDLC links, the communication controller CCL separates the data into buffers for each data validator DV and the supervisory processor SP.

To optimise the processing of data from high priority sites, the transfer of data to the data validator DV over the local area network is synchronised to the receipt of the last message from a high priority site (from all links). Polling for this data is synchronised to a half-second flag.

Messages received from any other central control processor are passed to a task which sets up additional data in the poll request data packets or interrupts the polling sequence to transmit higher priority packets in between poll requests. Down line loading of outstations database(s) is phased so that the polling sequence is not unduly delayed.

'WANTED' LIST HANDLING

A communication controller CCL only receives a message packet from a data validator DV for a 'Wanted' vehicle when an anomaly is detected at a high priority outstation. It is important to get that information to the outstation quickly—to display the data on a police terminal or to get a frame of a picture of the vehicle sent to the central control, so the poll request sequence is interrupted, to send a special 'wanted' vehicle data packet.

CONFIGURATION DATA HANDLING AND INITIALISATION

During communication controller CC initialisation, the configuration of all equipment under the control of that communication controller CCL is down-line loaded from the supervisory processor and stored in random access memory. This data includes the configured high priority and low priority outstation lists, communication systems addresses for each outstation (HDLC network) and central control processor local area network and the configuration data for each outstation (including interrogator and loop layout configuration).

Whenever an outstation is (re)initialised the communication controller CCL controls both the link set-up procedure and the down-line loading of data. If an outstation is being initialised whilst the system is active, there must be minimal interference with data retrieval from other outstations, so once down-line loading has started, the data packets are interleaved between low priority outstation poll requests (not delaying high priority polling).

REAL-TIME UPDATES

Whilst on-line, the changes to communication controller configuration data are:

a) Change of outstation priority, when a terminal is connected or disconnected; and

b) Change of data validator DV address on the local area network, if processors are substituted.

In the first case, the communication controller CCL simply changes the relevant outstation between the high and low priority lists. In the latter case, the supervisory processor SP sends update information to the communication controller CCL, which changes the relevant address for that data validator DV on the local area network.

FAULT DETECTION AND RECOVERY

Apart from carrying out self checks when requested and sending the results to the supervisory processor SP, a communication controller CCL monitors the HDLC links for faults. Each data packet sent to an outstation should be acknowledged by a reply data packet immediately. If the reply is corrupted, the frame check sequence fails to match, or no reply is received for any transmission within a timeout period, the communication controller CCL retransmits the packet up to twice more. If no acknowledgement is received by this time, the outstation is marked 'suspect faulty' and the poll sequence continues. A count of consecutive 'suspect fault' indications is maintained each time the outstation is polled, and is cleared when an acknowledgement is received. When the count reaches a limit of say 3, the outstation is marked 'faulty' and the SP informed. Once the supervisory processor SP has recorded the fault, it can only be cleared by an operator (in the Central Office) or engineer (from an outstation terminal).

DATA VALIDATORS

Concerning the data validators DV, their primary function is to validate vehicle data before preparation of invoices. The data validator DV receives individual vehicle ENP data from the communication controllers CCL and checks the identity and location of each vehicle before sending the accounting information to the accounts processor AP which records each vehicle's road usage and periodically invoices the owner.

In one arrangement of the system, accounting information is sent to the supervisory processor SP and then to the accounts processor AP over a direct serial link SL. In another arrangement of the system, accounts information is sent to the accounts processor AP over the inter-processor bus IPB.

Whenever the data validator DV fails to confirm the identity or location of a vehicle at a high priority site, it immediately sends a message back to that outstation OS. At a CCTV outstation this initiates transmission to the central office of a frame of a picture of the vehicle which is suspect. At a manned site the data on the suspect vehicle will be output to the police or maintenance terminal.

In addition, for all sites regardless of priority, if the data validator DV fails to confirm the location (outstation) or security code of the vehicle, the information (together with the last known location) is passed on to the supervisory processor SP which attempts to recover the situation ('Anomaly Processing') or iden-

tify 'suspect' vehicles. These are then added to a 'Wanted' list and also notified to the data validator DV.

Two types of anomaly are passed to the supervisory processor SP for further analysis: an invalid security code for an ENP, or an invalid location (outstation) when compared with the vehicle's last known location. Each of these anomalies may be caused by a vehicle apparently missing one or two outstations through 'rat runs', a faulty outstation, a faulty ENP on the vehicle, or a rogue vehicle whose ENP has been tampered with.

The supervisory processor requests vehicles to be marked as 'wanted' and whenever a data validator DV receives data for such a vehicle, it is sent on to the supervisory processor SP immediately. The data validation processing is illustrated in the flow diagram of Figure 4.

It is necessary to process individual vehicle information as fast as it is arriving at the central control CC, and to provide any control information for the outstations as quickly as possible. To achieve this, a distributed microprocessor system is employed which uses different levels responsible for different functions.

At the lowest level within the central control, communication controllers CCL poll outstations OS regularly to retrieve individual vehicle information from the road.

As previously mentioned, this information is then buffered for onward transmission to a data validator DV the selection of data validator DV being dependent upon the vehicle serial number.

A set of data validators DV check each vehicle's information in order to charge the owner for road usage related to the sites (outstations OS) passed. In order to handle 350,000 vehicles, each data validator DV is allocated part of the whole database (in the order of 40-50,000 vehicles, although this may be reduced if the local area network can handle more nodes easily). When data is received from a communication controller CCL it is quickly processed and the result passed on to either the accounts processor AP or the supervisory processor SP in accordance with whether the accounts processor interfaces the bus IPB or is served by a serial link SL from the supervisory processor SP respectively. The incidence of invalid data should be such as to keep the loading in the supervisory processor SL low compared to the loading on a data validator DV.

The advantages of using a number of small processors rather than one large one include:

a) Lower overall cost;

b) Lower maintenance costs;

c) Possibility of smaller system initially, with controlled build-up to a larger system;

d) Input-output load is distributed;

e) Any fault will affect only a part of the system;

f) No routine maintenance is required on the data validators DV;

g) The mechanical number/ENP serial number relationship need only be retained in those processors requiring it, i.e., data validators DV and supervisory processors SP, thereby maximising security by minimising accessibility of this information to operating staff.

OPERATION

As data packets are received from communication controllers CCL they are put into high and low priority queues, with the high priority queue being processed at the first available opportunity (when any current processing finishes), in case a response has to be returned to the outstation quickly.

Each vehicle's data are checked for:

i) Correct data validator DV (as routed through from the communication controller CC);

ii) Valid, commissioned ENP (enables access to the vehicle's current database information);

iii) Being 'wanted' (data sent on the supervisory processor SP immediately);

iv) Valid security code (if any); and

v) Valid location with reference to the last recorded location.

If the data was received from a high priority site and test (iii) succeeds or any of tests (i,ii,iv or v) fail, information is sent immediately to the outstation for appending to a display on a police terminal or to a display at the central control.

To speed the processing, ENPs are distributed evenly throughout each data validators DV memory and a simple mapping from the low order bits of the ENP serial number is used to minimise searches for the actual database entry to a maximum of 30 vehicles in each section. Also, table look-up techniques are applied to security code checking (byte orientated) and location-to-location movement validation, to optimise processing time.

MESSAGE HANDLING—SUPERVISORY PROCESSOR AND ACCOUNTS

Anomalies are passed on to the supervisory processor SP as soon as they are detected (one vehicle per packet) over the local area network. Data forwarded to the supervisory processor SP are the received ENP data and (provided the ENP existed in the DV database) the current database record for the vehicle.

Accounting information is accumulated in the data validator DV in a large buffer so that larger, infrequent packets can be forwarded to the accounts processor when either the data in the buffer reaches a pre-defined size or after a known time since reception of data from the last outstation. Apart from data validator DV initialisation (down line loading of data validator DV configuration and database information) the supervisory processor SP

sends the following information to a data validator DV:

a) Time synchronisation—a local area network packet broadcast to all central control processors to ensure real time synchronisation (the data validator DV needs time-of-day to send accounting information);

b) Add a vehicle to the 'Wanted List' together with a reason;

c) Remove an operator-wanted vehicle from the 'Wanted List';

d) Remove a data validator DV-anomoly from the 'Wanted List';

e) Data validated (sending back an anomaly which has been checked out by the SP);

f) Update vehicle database (sending back the most recent data after an anomaly has been corrected by analysing several consecutive packets in the supervisory processor SP);

g) Mark a location 'faulty';

h) Clear a 'faulty' indication;

i) Request a vehicle's current location (in response to an operator command at the supervisory processor SP);

j) Instructions to perform a self-check.

The last two require a specific reply to be sent to the supervisory processor SP. Processing of these data packets is handled at a lower priority than raw vehicle data.

REAL-TIME UPDATES

Whenever a vehicle's ENP data is validated (either directly in the data validator DV or via the anomaly processing in the supervisory processor SP), the current database record in the data validator DV is updated with current location and security code indication. The 'Wanted List' and 'Faulty Location' markers are also updated as and when directed by the supervisory processor SP.

A basic database change occurs when an ENP is commissioned. Here the supervisory processor SP controls the commissioning process and updates the data validator DV database before informing the fitting station that the ENP is accepted.

SUPERVISORY PROCESSOR

Considering the supervisory processor SP, one of its main functions is to commission new ENPs. New vehicle information is sent to the supervisory processor SP from a fitting station and it is checked against the existing database (to ensure there is no duplication of data). Valid data is then updated in the supervisory processor SP and the data validator DV and is sent back to the fitting station for confirmation by the operator. Upon receipt of the confirmation, the ENP is 'commissioned' and the system is ready to accept information from any location.

The supervisory processor SP, manages the resources of all central control CC processors and performs secondary functions that arise from DV data validator operations.

In one arrangement, the accounts processor AP does not interface to the local area network, so all accounting information is routed through the supervisory processor SP, which queues information on a disc store DS, and passes it serially over a 9600 baud direct link SL to the accounts processor AP. This arrangement is not necessary when the accounts processor AP interfaces to the local area network. The supervisory processor SP system is built around a disc-based operating system because this processor needs to:

a) Hold large amounts of data, for all levels of processor in the system;

b) Store vehicle data over quite long periods of time, for anomaly processing;

c) Handle operator communications, via several terminals and

d) Maintain information on system status and performance related to the many processors and their databases.

Operator communication OC facilities are provided via the supervisory processor SP, with two visual display units (VDU's) interfacing to the operators in the control room and one hard copy terminal upon which the supervisory processor SP logs all significant events.

The supervisory processor SP contains a real time clock which is used to maintain realtime (synchronised) in all other processors that require it, for example for accounting information, relating CCTV pictures to a time of day and accessing vehicle movements in time.

The supervisory processors SP re-validate ENP data whenever possible, identify equipment faults from ENP data analysis, manage database information, and provide information to the operators in a simple but effective way. The supervisory processor SP uses the local area network to ensure that communications between all central control CC processors are maintained and thus all of them are functioning correctly. Changes to system configuration (commissioning/de-commissioning of ENPs; switching to standby processors; adding new equipment or links) are all controlled by the supervisory processor SP system, so that the central store of all database information is kept up-to date on a disc DS.

The relationship between each vehicle's mechanical number plate (MNP) and ENP serial number is stored in the data validator DV (to identify the MNP from the ENP serial number) and in the supervisory processor SP. In the supervisory processor SP only, the inverse relationship is also held (on disc), with ENP being stored against MNP. This enables mapping from an operator-defined MNP to its corresponding ENP serial number. There is no need for any operator to know any vehicle's ENP serial number, thus ensuring security of this coded information.

ANOMOLY PROCESSING

When anomalies are received by the supervisory processor SP, it attempts to re-validate the data (security code, location or both). Initially invalid locations are checked using the vehicle's last known location, to discover whether the vehicle has passed through faulty outstations and to identify 'suspect' outstation equipment. If more than one non-faulty outstation exists between the two given locations, the vehicle is added to the 'Wanted List' and a record is kept of all its movements until an operator confirms re-validation.

Invalid security codes cannot be re-validated immediately, so a record is started which keeps track of the vehicle's security code changes and to continue validating the locations. If, after 3 security codes have been recorded, its position in the code sequence cannot be ascertained, the vehicle identity is added to the 'Wanted List' as for invalid locations.

For each subsequent recognition of a vehicle on the 'Wanted List' the data DV sends the latest information to the supervisory processor SP which adds it to the vehicle's record and attempts to re-validate the last 3, say, security code and location parameters. When a revalidation is achieved, the system informs the operator who can display the record of information and, optionally, clear the vehicle from the 'Wanted List'.

When data is re-validated (the supervisory processor SP ensures that both location and security code are correct), the latest data are passed back to the data validator DV to update its database and the vehicle is removed from the 'Wanted List' in both supervisory processor SP and data validator DV (unless required by the operator for other reasons).

A flow diagram of the anomoly processing/fraud identification is illustrated in Figure 5. Operator facilities OC are available to manipulate the 'Wanted List' and for fault management VDU terminals allow system messages to be displayed in a non-scrolling area of the screen, and operator information to be scrolled using the remainder of the screen.

CLAIMS

1. A data capture system for the automatic charging of tolls to vehicular users of roads, the capture system comprising, a plurality of vehicle identity data transmitting means each being individually attachable to vehicles, a plurality of roadside vehicle identity data interrogating means linked by a communications network with a central control which includes a plurality of communications control processors, and a plurality of vehicle identity data validating processors which communicate by means of a common inter-processor bus, wherein each data validating processor is allocated a discrete subset of all vehicles handled by the system and wherein upon transmitted vehicle identity data being detected by any one roadside vehicle identity data interrogating means, the vehicle identity data is transmitted through the communications network to a communications control processor and then by way of the common inter-processor bus to the particular data validating processor allocated to the subset of vehicles within which, the detected vehicle identity data is located, whereupon, the detected vehicle identity data is validated for use in enabling the preparation of toll invoices for despatch to the particular vehicle user concerned.

2. A data capture system as claimed in claim 1, in which the vehicle identity transmitting means is electronic number plate apparatus comprising a module incorporating storage means for storing the vehicle identity data and transmitting means for transmitting said vehicle identity data and wherein the vehicle identity data comprises for each individual electronic number plate apparatus, a code representing the unique serial number of the apparatus, the serial number being programmed into the storage means.

3. A data capture system as claimed in claim 2, in which the vehicle identity interrogating means is an outstation comprising an interrogator, a transmission unit, a processor and a plurality of interfaces to local equipment, wherein the outstation is connected to a plurality of inductive receive loops which are capable of electromagnetically coupling with the transmitting means enabling selection of the codes indicative of a vehicle's identity, the code signals being demodulated by the interrogator and passed to the processor for code verification, whereupon the verified code is transmitted from the outstation by the transmission unit.

4. A data capture system as claimed in claim 3, in which one local equipment comprises a closed circuit television (CCTV) system which stores frames of pictures of vehicles in a suspect category which are captured in the CCTV system, wherein the stored picture frames are transmitted to the central control for analysis and/or display upon a message, relating to vehicles in the suspect category, being transmitted from a communication controller to an outstation incorporating a CCTV system.

5. A data capture system as claimed in claim 4, in which the communications network is a cable network, wherein the network is arranged to link the outstations to an inter-processor high-speed bus at the control centre, under the control of the communication controllers and wherein each communications controller incorporates a plurality of outstation channels each of which is connected to a plurality of outstations wherein each communications controller is enabled to control a part of the complete cable network.

6. A data capture system as claimed in

claim 5, in which the data validating processors and a supervisory processor are connected to the inter-processor bus, wherein each data validating processor receives, from a communication controller, vehicle data comprising serial number, security code and location (outstation) concerned with its own allocated subset of vehicles exclusively for processing.

7. A data capture system as claimed in claim 6, in which the data validating processor is arranged to check that the serial number is in the range allocated to that particular data validation wherein when the check is not confirmed a message indicating an invalid serial number is sent to the supervisory processor.

8. A data capture system as claimed in claim 7, in which when the serial number check is confirmed, the memory location in the data validator holding the vehicle's data is determined wherein a check to determine if the electronic number plate identified is in commission, wherein if the check is not confirmed a message indicating an invalid serial number is sent to the supervisory processor.

9. A data capture system as claimed in claim 8, in which when the data validation processor determines that either the location (outstation) of the vehicle with respect to its last stored location is invalid or the security code with respect to the last stored security code is invalid, in each case respectively, a message is sent to the supervisory processor to initiate anomoly processing.

10. A data capture system as claimed in any of claims 7, 8 or 9 in which the vehicle data being processed is from a high priority outstation, a message is sent to that outstation to;

a) display the vehicle data at the police or maintenance terminal, or

b) to append the vehicle data to a frame of a picture of the vehicle.

11. A data capture system as claimed in claim 6, in which when the data validating processor determines the serial number location (outstation) and the security code are valid, the mechanical registration number and location are sent to an accounts processor for toll charging purposes.

12. A data capture system as claimed in claim 11 in which accounting information is routed through the supervisory processor, the accounting information being queued on a disc store and transmitted serially over a direct link to the accounts processor.

13. A data capture system as claimed in claim 11, in which the accounting information is routed over the inter-processor bus to the accounts processor.

14. A data capture system as claimed in claim 7, in which when the supervisory processor receives a message indicating an invalid serial number the supervisory processor arranges for the vehicle identity to be logged on a 'Wanted List'.

15. A data capture system as claimed in claim 9, in which upon the supervisory processor receiving anomoly data from the data validating processor the supervisory processor performs a process for revalidation of the data whereby in respect of invalid locations the vehicle's last location is checked against its current location to discover whether the vehicle passed through faulty outstations and if it is determined that more than one non-faulty outstation exists between two given locations the vehicle identity is logged on a 'Wanted List'.

16. A data capture system as claimed in claim 9, in which the supervisory processor receives anomoly data from the data validating processor, the supervisory processor performs a process for revalidation of the data, whereby a record is started which keeps track of the security code changes with continued validation of locations, and then following the recordal of three security codes the position in the code sequence can not be ascertained, the vehicle identity is logged on a 'Wanted List'.

17. A data capture system as claimed in claims 15 or 16, in which revalidated data from the supervisory processor is returned to the relevant data validation processor whereupon its records are updated and the vehicle identity is removed from the 'Wanted List'.

18. A data capture system as claimed in any one of claims 2 to 17, in which the storage means is a fuse-link PROM.

19. A data capture system as claimed in any one of claims 2 to 17, in which the transmitting means comprises an aerial.

20. A data capture system substantially as described herein, with reference to, and as shown, in the accompanying drawings.

Printed in the United Kingdom for
Her Majesty's Stationery Office, Dd 8818935, 1985, 4235.
Published at The Patent Office, 25 Southampton Buildings,
London, WC2A 1AY, from which copies may be obtained.